In the United States Patent and Trademark Office
Board of Patent Appeals and Interferences

Appeal Brief

In re the Application of:

Glen A. Jaquette
Serial No. 09/977,159
Filed: October 11, 2001
Attorney Docket No. TUC9001022US1

METHOD, SYSTEM, AND PROGRAM FOR SECURELY PROVIDING KEYS TO ENCODE AND DECODE DATA IN A STORAGE CARTRIDGE

Submitted by:

Konrad, Raynes & Victor LLP
315 So. Beverly Dr., Ste. 210
Beverly Hills CA 90212
(310) 556-7983
(310) 556-7984 (fax)

TABLE OF CONTENTS

I. Real Party in Interest

The entire right, title and interest in this patent application is assigned to real party in interest International Business Machines Corporation.

II. Related Appeals, Interferences, and Judicial Proceedings

Appellant, Appellant's legal representative, and Assignee are not aware of any other prior or pending appeals, interferences, and judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of the Claims

Claims 1-43 are pending and have been rejected.

The second final office action dated May 12, 2006 ("Second Final Office Action") of the claims is being appealed for all pending claims 1-43.

IV. Status of Amendments

No amendment to the claims was filed after receipt of the Second Final Office Action.

V. Summary of the Claimed Subject Matter

A. Independent Claim 1

Independent claim 1 is directed to a method for enabling access to data in a storage medium within one of a plurality of storage cartridges enabled to be mounted into an interface device. FIGs. 11, 12, and 13 and the corresponding discussion on para. [0048], pg. 19 through para. [0053], pg. 21 disclose an embodiment for a host 500 and interface device 502 to interact to enable access to one of a plurality of storage cartridges. FIGs. 14 and 15 and corresponding discussion at paras. [0055], pg. 21 through para. [0058], pg. 23, disclose an additional embodiment for a host 700 and data interface device 702 to interact to enable access to one of a plurality of storage cartridges. FIG. 16 and 17 and corresponding discussion at paras. [0059]-[0062], pgs. 23-25 disclose an additional embodiment for a host 800 and data interface device 802 to interact to enable access to a storage cartridge.

Claim 1 requires providing an association of at least one coding key to the plurality of storage cartridges. With respect to this claim requirement the Specification (para. [0047], pg. 19) discloses an MRU key 10 that is used to encode and decode data on at least one storage cartridge. The Specification further discloses (para. [0059], pgs. 23-24) that the host 800 maintains a key map 818 that associates one MRU key 810a., b...n with each storage cartridge 506a, b...n and that a single MRU key may be used for multiple storage cartridges 506a, b...n

Claim 1 further requires encrypting the coding key. With respect to this limitation, the Specification discloses (FIG. 12, block 552 and para. [0048], pg. 19) that the I/O manager 516 encrypts the MRU key 510 with the interface public key 512. The Specification further discloses (FIG. 15, block 754, para. [0056], pg. 22) that I/O manager 716 encrypts the MRU key 710 with the host public key (K_H). The Specification further discloses (FIG. 17, block 854 and para. [0061], pg. 24) that the I/O manager 816 encrypts the MRU key with the interface device public key (K_I).

Claim 1 further requires decrypting the encrypted coding key to use to decode and code data stored in the storage medium of at least one of the storage cartridges. With respect to this requirement, the Specification discloses (FIG. 13, blocks 630 and 632, para. [0051], pg. 20) that the interface device 502 decrypts the encrypted MRU key to use to encode data being written to the storage cartridges. The Specification discloses (FIG. 15, blocks 776 and 778, para. [0057], pg. 22) that the controller 718 decrypts the encrypted MRU key to use to encrypt and/or decrypt data. The Specification further discloses (FIG. 17, blocks 864 and 866, para. [0062], pgs. 24-25) that the controller 820 uses the interface private key to decrypt the encrypted MRU key.

B. Independent Claim 10

Independent claim 10 is directed to a method performed by an interface device for accessing data in a removable storage cartridge including a storage medium coupled to the interface device. The Specification discloses (FIG. 13 and para. [0050]-[0051], pg. 20; FIG. 15 and para. [0056]-[0057], pg. 22; FIG. 17 and paras. [0061] to [0062]) an embodiment of operations the interface device 502, 702, 802 performs to access a removable storage cartridge 506a…506n

Claim 10 requires receiving an encrypted coding key from a host system. With respect to this limitation, the Specification discloses (FIG. 12, blocks 570, 574 and para. [0049], pg. 20; FIG. 15, block 770, para. [0057], pg. 22; FIG. 17, block 860, para. [0062], pgs. 24-25) that the interface device 502, 702, 802 receives the encrypted MRU key. Claim 10 further requires decrypting the encrypted coding key. With respect to this limitation, the Specification discloses (FIG. 13, block 630, para. [0051], pg. 20; FIG. 15, block 776, para. [0057], pg. 22; FIG. 17, block 864, para. [0062], pgs. 24-25) that the interface device 502, 702, 802 decrypts the encrypted MRU key.

Claim 10 further requires using the coding key to encode data to write to the storage medium and using the coding key to decode data written to the storage medium. With respect to these limitations, the Specification discloses (FIG. 13, block 632, para. [0051], pg. 20; FIG. 15, block 778, para. [0057], pg. 22; and FIG. 17, block 866, para. [0062], pgs. 24-25) that the interface device 502, 702, 802 uses the MRU key to encode and decode data to perform the I/O request, read or write, to the target storage cartridge.

C. Independent Claim 18

Independent claim 18 is directed to a system for enabling access to data in a storage medium within one of a plurality of storage cartridges enabled to be mounted into an interface device. FIGs. 11, 12, and 13 and the corresponding discussion on para. [0048], pg. 19 through para. [0053], pg. 21 disclose an embodiment for a host 500 and controller 502 to interact to enable access to one of a plurality of storage cartridges. FIGs. 14 and 15 and corresponding discussion at paras. [0055], pg. 21 through para. [0058], pg. 23, disclose an additional embodiment for a host 700 and data interface device 702 to interact to enable access to one of a plurality of storage cartridges. FIG. 16 and 17 and corresponding discussion at paras. [0059]-[0062], pgs. 23-25 disclose an additional embodiment for a host 800 and data interface device 802 to interact to enable access to a storage cartridge.

Claim 18 further requires an interface device at which the storage cartridges are enabled to be mounted, wherein the interface device is enabled to write data to the storage medium within the storage cartridges and reading data from the storage medium in the storage cartridges. FIG. 10 of the Specification discloses a data interface device 502 providing read/write access to one of a plurality of data storage cartridges 506a…n mounted in the interface device. (Specification, FIG. 10, para. [0043]-[0044], pgs. 17-18). Interface devices 502, 702, and 802 are disclosed in FIGs. 11, 14, and 16 and para. [0047], pg. 19; para. [0055], pgs. 21-22; and para. [0059], pgs. 23-24.

Claim 18 further requires a means for providing an association of at least one coding key to the plurality of storage cartridges. With respect to this claim requirement the Specification (at para. [0047], pg. 19) discloses an MRU key 10 that is used to encode and decode data on at least one storage cartridge. The Specification further discloses (at para. [0059], pgs. 23-24) that the host 800 maintains a key map 818 that associates one MRU key 810a., b...n with each storage cartridge 506a, b...n and that in alternative implementations, a single MRU key may be used for multiple storage cartridges 506a, b...n If this limitation is construed as a means-plus-function limitation, then the structure and acts corresponding to this claimed function comprises the host 800 that maintains a key map 818 associating storage cartridges with MRU keys and equivalents thereof.

Claim 18 further requires a means for encrypting the coding key. With respect to this limitation, the Specification discloses (FIG. 12, block 552 and para. [0048], pg. 19) that the I/O manager 516 encrypts the MRU key 510 with the interface public key 512. The Specification further discloses (FIG. 15, block 754, para. [0056], pg. 22) that I/O manager 716 encrypts the MRU key 710 with the host public key (K_H). The Specification further discloses (FIG. 17, block 854 and para. [0061], pg. 24) that the I/O manager 816 encrypts the MRU key with the interface device public key (K_I). If this limitation is construed as a means-plus-function limitation, then the structure and acts corresponding to this claimed function comprises the I/O manager 516, 716, 816 that encrypts the MRU key and equivalents thereof.

Claim 18 further requires decrypting the encrypted coding key to use to decode and code data stored in the storage medium of at least one of the storage cartridges. With respect to this requirement, the Specification discloses (FIG. 13, blocks 630 and 632, para. [0051], pg. 20) that the interface device 502 decrypts the encrypted MRU key to use to encode data being written to the storage cartridges. The Specification discloses (FIG. 15, blocks 776 and 778, para. [0057], pg. 22) that the controller 718 of the interface device 702 decrypts the encrypted MRU key to use to encrypt and/or decrypt data. The Specification further discloses (FIG. 17, blocks 864 and 866, para. [0062], pgs. 24-25) that the controller 820 of the interface device 802 uses the interface private key to decrypt the encrypted MRU key.

D. Independent Claim 23

Independent claim 23 is directed to a system for accessing data in a removable storage cartridge including a storage medium coupled to the interface device. The Specification discloses (FIG. 13 and para. [0050]-[0051], pg. 20; FIG. 15 and para. [0056]-[0057], pg. 22; FIG. 17 and paras. [0061] to [0062]) an embodiment of an interface device 502, 702, 802 that performs operations to access a removable storage cartridge 506a…506n

Claim 23 requires an interface device enabled to be coupled to the removable storage cartridge to access data in the removable storage cartridge, wherein the interface device causes operations to be performed. FIG. 10 of the Specification discloses a data interface device 502 providing read/write access to one of a plurality of data storage cartridges 506a…n mounted in the interface device. (Specification, FIG. 10, para. [0043]-[0044], pgs. 17-18). Interface devices 502, 702, and 802 are disclosed in FIGs. 11, 14, and 16 and para. [0047], pg. 19; para. [0055], pgs. 21-22; and para. [0059], pgs. 23-24.

Claim 23 further requires that the interface device receive an encrypted coding key from a host system. With respect to this limitation, the Specification discloses (FIG. 12, blocks 570, 574 and para. [0049], pg. 20; FIG. 15, block 770, para. [0057], pg. 22; FIG. 17, block 860, para. [0062], pgs. 24-25) that the interface device 502, 702, 802 receives the encrypted MRU key. Claim 23 further requires that the interface device decrypt the encrypted coding key. With respect to this limitation, the Specification discloses (FIG. 13, block 630, para. [0051], pg. 20; FIG. 15, block 776, para. [0057], pg.

22; FIG. 17, block 864, para. [0062], pgs. 24-25) that the interface device 502, 702, 802 decrypts the encrypted MRU key.

Claim 23 further requires that the interface device use the coding key to encode data to write to the storage medium and using the coding key to decode data written to the storage medium. With respect to this limitation, the Specification discloses (FIG. 13, block 632, para. [0051], pg. 20; FIG. 15, block 778, para. [0057], pg. 22; and FIG. 17, block 866, para. [0062], pgs. 24-25) that the interface device 502, 702, 802 uses the MRU key to encode and decode data to perform the I/O request, read or write, to the target storage cartridge.

E. Independent Claim 27

Independent claim 27 is directed to an article of manufacture including code for enabling access to data in a storage medium within one of a plurality of storage cartridges enabled to be mounted into an interface device. FIGs. 11, 12, and 13 and the corresponding discussion on para. [0048], pg. 19 through para. [0053], pg. 21 disclose an embodiment for a host 500 and controller 502 to interact to enable access to one of a plurality of storage cartridges. FIGs. 14 and 15 and corresponding discussion at paras. [0055], pg. 21 through para. [0058], pg. 23, disclose an additional embodiment for a host 700 and data interface device 702 to interact to enable access to one of a plurality of storage cartridges. FIG. 16 and 17 and corresponding discussion at paras. [0059]-[0062], pgs. 23-25 disclose an additional embodiment for a host 800 and data interface device 802 to interact to enable access to a storage cartridge. The Specification discloses (para. [0069], pg. 27) that an "article of manufacture" refers to code or logic in which the embodiments are implemented.

Claim 27 requires providing an association of at least one coding key to the plurality of storage cartridges. With respect to this claim requirement the Specification (at para. [0047], pg. 19) discloses an MRU key 10 that is used to encode and decode data on at least one storage cartridge. The Specification further discloses (at para. [0059], pgs. 23-24) that the host 800 maintains a key map 818 that associates one MRU key 810a., b...n with each storage cartridge 506a, b...n and that in alternative implementations, a single MRU key may be used for multiple storage cartridges 506a, b...n

Claim 27 further requires encrypting the coding key. With respect to this limitation, the Specification discloses (FIG. 12, block 552 and para. [0048], pg. 19) that the I/O manager 516 encrypts the MRU key 510 with the interface public key 512. The Specification further discloses (FIG. 15, block 754, para. [0056], pg. 22) that I/O manager 716 encrypts the MRU key 710 with the host public key (K_H). The Specification further discloses (FIG. 17, block 854 and para. [0061], pg. 24) that the I/O manager 816 encrypts the MRU key with the interface device public key (K_I).

Claim 27 further requires decrypting the encrypted coding key to use to decode and code data stored in the storage medium of at least one of the storage cartridges. With respect to this requirement, the Specification discloses (FIG. 13, blocks 630 and 632, para. [0051], pg. 20) that the controller 502 decrypts the encrypted MRU key to use to encode data being written to the storage cartridges. The Specification discloses (FIG. 15, blocks 776 and 778, para. [0057], pg. 22) that the controller 718 decrypts the encrypted MRU key to use to encrypt and/or decrypt data. The Specification further discloses (FIG. 17, blocks 864 and 866, para. [0062], pgs. 24-25) that the controller 820 uses the interface private key to decrypt the encrypted MRU key.

F. Independent Claim 36

Independent claim 36 is directed to an article of manufacture including code executed in an interface device for accessing data in a removable storage cartridge including a storage medium coupled to the interface device. The Specification discloses (FIG. 13 and para. [0050]-[0051], pg. 20; FIG. 15 and para. [0056]-[0057], pg. 22; FIG. 17 and paras. [0061] to [0062]) an embodiment of operations the interface device 502, 702, 802 performs to access a removable storage cartridge 506a…506n. The Specification discloses (para. [0069], pg. 27) that an "article of manufacture" refers to code or logic in which the embodiments are implemented.

Claim 36 requires receiving an encrypted coding key from a host system. With respect to this limitation, the Specification discloses (FIG. 12, blocks 570, 574 and para. [0049], pg. 20; FIG. 15, block 770, para. [0057], pg. 22; FIG. 17, block 860, para. [0062], pgs. 24-25) that the interface device 502, 702, 802 receives the encrypted MRU key. Claim 36 further requires decrypting the encrypted coding key. With respect to this limitation, the Specification discloses (FIG. 13, block 630, para. [0051], pg. 20; FIG. 15, block 776, para. [0057], pg. 22; FIG. 17, block 864, para. [0062], pgs. 24-25) that the interface device 502, 702, 802 decrypts the encrypted MRU key.

Claim 36 further requires using the coding key to encode data to write to the storage medium and using the coding key to decode data written to the storage medium. With respect to these limitations, the Specification discloses (FIG. 13, block 632, para. [0051], pg. 20; FIG. 15, block 778, para. [0057], pg. 22; and FIG. 17, block 866, para. [0062], pgs. 24-25) that the interface device 502, 702, 802 uses the MRU key to encode and decode data to perform the I/O request, read or write, to the target storage cartridge.

VI. Grounds of Rejection to Be Reviewed on Appeal

A concise statement listing each ground of rejection presented for review is as follows:

A. Claims 1-43 are rejected under 35 U.S.C. §102(e) as being unpatentable over Kuroda (U.S. Patent No. 6,915,434).

VII. Argument

A. Rejection Under 35 U.S.C. §102(e) as Anticipated by Kuroda

1. Claims 1, 2, 4, 5, 18, 19, 21, 22, 27, 28, 30, and 31

The Examiner cited FIGs. 1, 2, 11, 13, 16, 22, 23, and 25 and the accompanying text of Kuroda as teaching the requirements of claims 1, 18, and 27. (Second Final Office Action, pg. 2)

In the Response dated February 8, 2006, Applicants ("Feb. 2006 Response"), Applicants requested that the Examiner cite to specific sections of the cited references that disclose the independent claim requirements, instead of a general citation to nine figures and their accompanying text which spans several columns of the cited patent. Applicants noted the requirements of 37 CFR 1.104(c)(2):

> When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable.

See, also, MPEP 707, pg. 700-111, (Rev. 5, Aug. 2006).

Notwithstanding Applicants request, the Examiner in the following Second Final Office Action, which is the subject of this Appeal, ignored this request. Accordingly, Applicants submit that the Examiner action does not comply with the requirements of 37 CFR 1.104(c)(2) as the particular parts relied on were not designated as nearly as practicable.

Applicants further submit that a review of the cited FIGs. 1, 2, 11, 13, 16, 22, 23, and 25 and the accompanying text of Kuroda reveals that Kuroda does not disclose the claim requirements, and, that the rejection should also be overturned for these substantive reasons.

Claims 1, 18, and 27 concern enabling access to data in a storage medium within one of a plurality of storage cartridges capable of being mounted into an interface device and require: providing an association of at least one coding key to the plurality of storage cartridges; encrypting the coding key; and decrypting the encrypted coding key to use to decode and code data stored in the storage medium of the at least one of the storage cartridges.

Thus, the claims require that a coding key associated with a plurality of storage cartridges is encrypted and then decrypted to use to decode and code data stored in at least one of the storage cartridges.

Applicants submit that the below review reveals that the cited FIGs. 1, 2, 11, 13, 16, 22, 23, and 25 and the accompanying text does not disclose these claim requirements. This below review shows that the general concept of the cited Kuroda mentions two keys, an "individual key" and a "group key". The "individual key" is unique to a storage apparatus and used to encrypt and decrypt data in the storage unit. The "group key" is used to encrypt data unencrypted with the "individual key" that is being transmitted between storage apparatuses in the same group. These cited keys of Kuroda do not disclose a coding key associated with a plurality of storage cartridges that is encrypted, decrypted and then used use to decode and code data stored in at least one of the storage cartridges.

The cited FIG. 1 shows a key management unit 2 and encryption unit 3 for a storage apparatus. (Kuroda, col. 5, lines 33-50) The encrypting unit 3 encrypts data using an "individual key" stored in the storage apparatus that is unique to the apparatus. The cited FIG. 2 shows a configuration of the storage apparatus that stores three types of keys, an "individual key" unique to the apparatus, a "group key", and a public key used when data is transmitted to another group. (Kuroda, col. 5, line 50 to col. 6, line 9). The cited FIG. 11 concerns a configuration of the storage apparatus that has a master key storage unit storing a master key which is a common key shared by all apparatuses. (Kuroda, col. 9, lines 35-43) The cited FIG. 13 discusses how to generate a group key. (Kuroda, col. 10, lines 6-24) The cited FIG. 16 shows communication between groups of the storage apparatuses. (Kuroda, col. 10, line 65 to col. 11, line 17). The cited FIG. 22 shows a method for generating a key, including using the group ID to generate a group key. (Kuroda, col. 12, lines 51-67). The cited FIG. 23 shows the generation and distribution of the group key. (Kuroda, col. 13, lines 1-27). The cited FIG. 25 shows how a program is loaded to realize the storage apparatus. (Kuroda, col. 13, line 52 to col. 14, line 10)

Applicants submit that the Examiner has failed to show specifically where any of the above cited figures and their accompanying text discloses that a coding key associated with a plurality of storage cartridges is encrypted and decrypted to use to decode and code data stored in the storage medium of at least one of the storage cartridges.

Neither the cited "group key" nor "individual key" comprises a coding key that is encrypted and decrypted to use to decode and code data. The cited "group key" of Kuroda is used to encrypt data being transmitted and received between storage apparatuses in the same group. (Kuroda, col. 6, lines 25-33; col. 9, lines 10-15). The Examiner has not shown where Kuroda discloses that the "group key" is itself encrypted and decrypted and then used to decode and code data to the storage medium in a storage cartridge as claimed. The cited "individual key" is unique to a storage apparatus and used to encrypt and decrypt data for that storage apparatus. (Kuroda, col. 7, lines 53-65).

Although the "individual key", unique to a storage apparatus, is used to encrypt data, the Examiner has not shown where Kuroda discloses that the "individual key" is itself encrypted and decrypted and then used to decode and code data as claimed. Further, the Examiner has not shown where the cited "individual key" is associated with a plurality of storage cartridges. In fact, Kuroda's emphasis that the "individual key" is unique to the storage apparatus teaches away from this claim requirement.

Applicants submit that other sections of Kuroda emphasize these differences of the cited individual and group keys and the claimed coding key. For instance, Kuroda mentions in numerous instances, including the Abstract, Summary of the Invention, independent claims, and Specification that the cited "individual key" is "unique" to the storage apparatus. (Kuroda, Abstract, line 2; claim 1, col. 14, line 26-30; col. 2, lines 24-28, 34-37; col. 3, lines 33-38, 48-51, 60-63; col. 3, lines 67 to col. 4, line 1; col. 4, lines 10-12; col. 5, lines 27-29, 33-35, 45-57, 62-64). Thus, the cited Kuroda teaches away from the "individual key" being a coding key associated with a plurality of storage cartridges. Further, the Examiner has not cited any part of Kuroda that discloses that the "individual key" is encrypted and decrypted to use to decode and code data.

Yet further, Kuroda describes the "individual key" as associated with one "electronic data storage apparatus". Kuroda mentions that the "electronic data storage apparatus comprises a data storage unit for storing electronic data". (Kuroda, col. 6, lines 3-8). However, the claims require a coding key associated with storage cartridges. Applicants submit that the cited "electronic data storage apparatus" of Kuroda does not disclose the claim requirement of a storage cartridge having the storage medium because the "electronic data storage apparatus" of Kuroda is the storage drive performing the writing and encryption, not a storage cartridge to be mounted having the storage medium on which the data is written, as required by the claims.

In the Response to Arguments, the Examiner discussed the operations of Kuroda's "individual key" and "common key", which is another term used for the "group key", or key used to encrypt data being transmitted. ("A group key storage unit 15 stores a group key as a common key in a group of a plurality of electronic data storage apparatuses 10", col. 5, lines 54-67). The Examiner found that:

> The encryption unit performs an encrypting process using an individual key on the electronic data stored in the electronic data storage apparatus to which it belongs, and performs an encrypting process or data verification using a common key on the electronic data transmitted to and received from other electronic data storage apparatus.

(Second Final Office Action, pg. 8).

This restatement of the operations of the "individual key" and common or group key still fails to disclose the claim requirements of a coding key associated with a plurality of storage cartridges that is also encrypted and decrypted to use to decode and code data stored in the storage medium of at least one of the storage cartridges.

For all the above reasons, Applicants request the Board to reverse the rejection of claims 1, 18, and 27.

Applicants submit that claims 2, 4, 5, 19, 21, 22, 28, 30, and 31 are patentable over the cited art because they depend from one of claims 1, 18, and 27, which are patentable over the cited art for the reasons discussed above and because the additional requirements of these claims in combination with the base claims provide further grounds of patentability over the cited art.

2. Claims 3, 20, and 29

Claims 3, 20, and 29 depend from claims 1, 18, and 27, and further require that the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key is enabled to be used to encode data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

The Examiner cited the same FIGs. 1, 2, 11, 13, 16, 22, 23, 25 and accompanying text in Kuroda discussed above with respect to the independent claims as disclosing the additional requirements of claims 3, 20, and 29. (Second Final Office Action, pg. 3)

Applicants submit that the Examiner has not cited any part of Kuroda that discloses that one key associated with a plurality of storage cartridges is used to encode and decode to the storage mediums of a plurality of storage cartridges. The above discussed "group key" is used to encrypt and decrypt data being transmitted between storage apparatuses. (Kuroda, col. 7, lines 53-65) The cited "individual key" unique to each storage apparatus is used to encrypt and decrypt data on the storage apparatus. Thus, this "individual key" cannot disclose the claim requirement of a key to encode and decode data written to a plurality of storage mediums of a plurality of storage cartridges.

Yet further, the Examiner has not cited any part of Kuroda that discloses associating keys with storage cartridges. Instead, Kuroda discusses keys associated with "electronic data storage apparatus" used to perform the reading and writing to storage media.

Accordingly, Applicants request the Board to reverse the rejection of claims 3, 20, and 29 because the additional requirements of these claims are not disclosed in the cited Kuroda.

3. Claims 6 and 32

Claims 6 and 32 depend from claims 1 and 27 and further require transmitting the encrypted coding key to the interface device, wherein the interface device decrypts the coding key to use to decode and code data stored in the storage medium.

The Examiner cited the same FIGs. 1, 2, 11, 13, 16, 22, 23, 25 and accompanying text in Kuroda discussed above with respect to the independent claims as disclosing the additional requirements of claims 6 and 32. (Second Final Office Action, pgs. 3-4)

As discussed, the cited "individual key" is used to encrypt and decrypt data for one "unique" storage apparatus. Applicants submit that the Examiner has not cited any part of Kuroda that discloses that this cited "individual key" is transmitted to an interface device into which a plurality of storage cartridges are mounted, where the interface device decrypts the coding key to decode and code data in the storage medium. Further, the Examiner has not cited where Kuroda discloses that the cited "group key" is encrypted and transmitted to an interface device into which a plurality of storage cartridges are mounted, where the "group key" is decrypted and used to code and decode data in the storage medium. Instead, the cited group key is used to transmit data between storage apparatuses in the group

Accordingly, Applicants request the Board to reverse the rejection of claims 6 and 32.

4. Claims 7 and 33

Claims 7 and 33 depend from claims 6 and 32 and further require that encrypting the coding key further comprises encrypting the coding key with a first key, wherein a second key used by the interface device enabled to decrypt the coding key encrypted with the first key.

The Examiner cited the same FIGs. 1, 2, 11, 13, 16, 22, 23, 25 and accompanying text in Kuroda discussed above with respect to the independent claims as disclosing the additional requirements of claims 7 and 33. (Second Final Office Action, pgs. 4)

Applicants submit that the Examiner has not cited any part of Kuroda that discloses that either the cited "individual key" or "group key" is encrypted with a first key and that the interface device is enabled to use a second key to decrypt the "individual key" or "group key", encrypted with the first key.

Accordingly, Applicants request the Board to reverse the rejection of claims 7 and 33.

5. Claims 8 and 34

Claims 8 and 34 depend from claims 6 and 32, respectively, and further require that encrypting the coding key further comprises encrypting the coding key with a first key, wherein a second key enabled to decrypt the coding key encrypted with the first key; encrypting the second key with a third key, wherein a fourth key used by the interface device enabled to decrypt data encrypted with the third key; and transmitting the coding key encrypted with the first key and the second key encrypted with the third key to the interface device.

The Examiner cited the same FIGs. 1, 2, 11, 13, 16, 22, 23, 25 and accompanying text in Kuroda discussed above with respect to the independent claims as disclosing the additional requirements of claims 8 and 34. (Second Final Office Action, pgs. 4)

Applicants submit that the Examiner has not cited any part of Kuroda that discloses that either the "individual key" or "group key" is encrypted with a first key, where a second key is enabled to decrypt the "individual key" or "group key" encrypted with the first key. Further, the Examiner has not cited any part of Kuroda that discloses that such second key is encrypted with a third key, where a fourth key is used by the interface device enabled to decrypt data encrypted with the third key. Yet further, the Examiner has not cited any part of Kuroda that discloses that the coding key, corresponding to the cited "individual key" or "group key", is transmitted encrypted with the first key and the second key encrypted with the third key to an interface device. Applicants submit that the Examiner has not cited where Kuroda discloses these specific encryption requirements involving three keys.

Accordingly, Applicants request the Board to reverse the rejection of claims 8 and 34.

6. Claims 9 and 35

Claims 9 and 35 depend from claims 6 and 32 and further require that encrypting the coding key further comprises: encrypting the coding key with a first key, wherein a second key enabled to decrypt the coding key encrypted with the first key; transmitting the coding key encrypted with the first key to the interface device; receiving, from the interface device, the coding key encrypted with the first key; decrypting the coding key with the second key; encrypting the coding key with a third key, wherein a fourth key used by the interface device enabled to decrypt data encrypted with the third key; and transmitting the coding key encrypted with the third key to the interface device.

The Examiner cited the same FIGs. 1, 2, 11, 13, 16, 22, 23, 25 and accompanying text in Kuroda discussed above with respect to the independent claims as disclosing the additional requirements of claims 8 and 34. (Second Final Office Action, pgs. 4)

Applicants submit that the Examiner has not cited any part of Kuroda that discloses that either the "individual key" or "group key", likened by the Examiner to the claimed coding key, is encrypted with a first key, where a second key is enabled to decrypt the "individual key" or "group key", encrypted with the first key. Further, the Examiner cited has not cited any part of Kuroda that discloses transmitting the "individual key" or "group key", or that an interface decrypts the cited "individual key" or "group key", likened to the claimed coding key, with a second key. Yet further, Examiner has not cited any part of Kuroda that discloses that the cited "individual key" or "group key" is yet further encrypted with a third key, where a fourth key used by the interface device is enabled to decrypt data encrypted with the third key. Applicants submit that the Examiner has not cited where Kuroda discloses these specific encryption requirements involving four keys.

Accordingly, Applicants request the Board to reverse the rejection of claims 9 and 35.

7. Claims 10, 11, 14, 23, 25, 36, 37, and 40

Independent claims 10, 23, and 36 concern an interface device for accessing data in a removable storage cartridge including a storage medium coupled to the interface device and require: receiving an encrypted coding key from a host system; decrypting the encrypted coding key; using the coding key to encode data to write to the storage medium; and using the coding key to decode data written to the storage medium.

The Examiner cited the same FIGs. 1, 2, 11, 13, 16, 22, 23, 25 and accompanying text in Kuroda discussed above with respect to the independent claims as disclosing the requirements of these claims. (Final Office Action, pg. 5).

As discussed, the above discussed Kuroda discusses how each storage apparatus has an "individual key" to encrypt data to the apparatus and uses a group or public key to encrypt data for transfer to another storage apparatus. Applicants submit, for the reasons discussed above, that the Examiner has not cited any part of Kuroda that discloses that an interface device to which removable cartridges are coupled receives an encrypted coding key from a host system, decrypts the key and then uses the key to code and decode data in a removable storage cartridge. Instead, the above cited Kuroda discusses how an "electronic data storage apparatus" uses a unique "individual key" to encrypt data written to the storage or transmitted. The Examiner has not cited any part of Kuroda that discloses that the "individual key" or "group key" are decrypted by an interface device and then used to encode and decode data written to the storage medium as claimed.

Accordingly, Applicants request the Board to reverse the rejection of claims 10, 23, and 36.

Applicants submit that claims 11, 14, 25, 37, and 40 are patentable over the cited art because they depend from one of claims 10, 23, and 36, which are patentable over the cited art for the reasons discussed above and because the additional requirements of these claims in combination with the base claims provide further grounds of patentability over the cited art.

8. Claims 12, 24, and 38

Claims 12, 24, and 38 depend from claims 10, 23, and 36, respectively, and further require that the coding key is encrypted by a first key maintained at the host system and maintaining a second key that enabled to decrypt data encrypted using the first key, wherein the second key is used to decrypt the coding key encrypted with the first key.

The Examiner cited the same FIGs. 1, 2, 11, 13, 16, 22, 23, 25 and accompanying text in Kuroda discussed above with respect to the independent claims as disclosing the additional requirements of claims 12, 24, and 38. (Second Final Office Action, pgs. 5)

Applicants submit that the Examiner has not cited any part of Kuroda that discloses that either the "individual key" or "group key" is encrypted with a first key and that the interface device is enabled to use a second key to decrypt the "individual key" or "group key", encrypted with the first key.

Accordingly, Applicants request the Board to reverse the rejection of claims 12, 24, and 38 because the additional requirements of these claims are not disclosed in the cited Kuroda.

9. Claims 13 and 39

Claims 13 and 39 depend from claims 12 and 38, respectively, and further require that the second key is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key.

The Examiner cited the same FIGs. 1, 2, 11, 13, 16, 22, 23, 25 and accompanying text in Kuroda discussed above with respect to the independent claims as disclosing the additional requirements of claims 13 and 39. (Second Final Office Action, pgs. 6)

Applicants submit that the Examiner has not cited any part of Kuroda that discloses that a second key used to decrypt the coding key, which the Examiner likens to the "individual key" and "group key", is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key. The discussion of the use of the "individual key" and "group key" in the cited Kuroda nowhere discloses how a claimed second key used to decrypt the coding is stored and accessed by decrypting logic as claimed.

Accordingly, Applicants request the Board to reverse the rejection of claims 13 and 39 because the additional requirements of these claims are not disclosed in the cited Kuroda.

10. Claims 15, 26, and 41

Claims 15, 26, and 41 depend from claims 12, 24, and 38, respectively, and further require: storing the coding key encrypted with the first key within the storage cartridge; receiving an input/output (I/O) request directed to the storage cartridge; and accessing the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

The Examiner cited the same FIGs. 1, 2, 11, 13, 16, 22, 23, 25 and accompanying text in Kuroda discussed above with respect to the independent claims as disclosing the additional requirements of claims 15, 26, and 41. (Second Final Office Action, pgs. 6)

Applicants submit that the Examiner has not cited any part of Kuroda that discloses storing the coding key in a storage cartridge, where the coding key is used to encrypt and decrypt data written to that same storage cartridge. In fact, Kuroda teaches away from this claim requirement because Kuroda mentions that an individual key storage unit 14 stores an "individual key" unique the electronic data storage apparatus 10. (Kuroda, col. 5, lines 63-64) The Examiner has not shown that the "individual key" is used to encrypt and decrypt data written to such individual key storage unit 14. Instead, Kuroda mentions that the "individual key" is unique to the electronic data storage apparatus. (Kuroda, col. 5, lines 63-65). Consequentially, the "individual key" of Kuroda, which is likened to the claimed coding key, would also not be accessed from a storage cartridge to which the data encrypted and decoded by the coding key is written, because Kuroda mentions that the "individual key" is stored in the individual key storage unit 14.

Accordingly, Applicants request the Board to reverse the rejection of claims 15, 26, and 41 because the additional requirements of these claims are not disclosed in the cited Kuroda.

11. Claims 16 and 42

Claims 16 and 42 depend from claims 10 and 36, respectively, and further require that the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key that is enabled to decrypt data encrypted using the first key. These claims further require: receiving, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is decrypted using a fourth key; accessing the fourth key; using the fourth key to decrypt the encrypted second key received from the host system; and using the decrypted second key to decrypt the received coding key encrypted using the first key.

The Examiner cited the same FIGs. 1, 2, 11, 13, 16, 22, 23, 25 and accompanying text in Kuroda discussed above with respect to the independent claims as disclosing the additional requirements of claims 15, 26, and 41. (Second Final Office Action, pgs. 6-7)

Applicants submit that the Examiner has not cited any part of Kuroda that discloses that the "individual" key or "group key" of Kuroda, which the Examiner likens to the claimed coding key, is encrypted by a first key and that a second key is enabled to decrypt data encrypted using the first key. Further, the Examiner has not cited any part of Kuroda that discloses the use of a third key to encrypt the second key that is decrypted using a fourth key, where the fourth key is used to decrypt the encrypted second key and the second key is used to decrypt the received coding key. Yet further, the Examiner has not cited any part of Kuroda disclosing the encryption of the individual or group key using first, second, third and fourth keys as claimed.

Accordingly, Applicants request the Board to reverse the rejection of claims 16 and 42 because the additional requirements of these claims are not disclosed in the cited Kuroda.

12. Claims 17 and 43

Claims 17 and 43 depend from claims 10 and 36, respectively, and further require that the coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key that is enabled to decrypt data encrypted using the first key. These claims further require: transmitting the encrypted coding key received from the host system back to the host system; in response to transmitting the encrypted coding key back to the host system, receiving, from the host system, the coding key encrypted using a third key, wherein data encrypted using the third key is decrypted using a fourth key; and accessing the fourth key, wherein the coding key is decrypted using the fourth key.

The Examiner cited the same FIGs. 1, 2, 11, 13, 16, 22, 23, 25 and accompanying text in Kuroda discussed above with respect to the independent claims as disclosing the additional requirements of claims 15, 26, and 41. (Second Final Office Action, pg. 7)

The Examiner has not cited any part of Kuroda that discloses the "individual key" or "group key" of Kuroda, which the Examiner likens to the claimed coding key, is encrypted by a first key and that a second key is enabled to decrypt data encrypted using the first key. Further, the Examiner has not cited any part of Kuroda that discloses that the individual or group key received from a host system is transmitted back to the host system and then the coding key is received from that host system encrypted using a third key.

Further, the Examiner has not cited any part of Kuroda that discloses the use of a third key to encrypt the second key, where the fourth key is used to decrypt he data encrypted with the third key. Yet further, the Examiner has not cited any part of Kuroda that discloses that a fourth key is used to decrypt the cited individual or group key, likened by the Examiner to the claimed coding key. Further, the Examiner has not cited any part of Kuroda that discloses the encryption of the individual or group key using first, second, third and fourth keys as claimed.

Accordingly, Applicants request the Board to reverse the rejection of claims 17 and 43 because the additional requirements of these claims are not disclosed in the cited Kuroda.

VIII. Conclusion

Each of the rejections set forth in the Second Final Office Action is improper and should be reversed.

Respectfully submitted,

/David Victor/

David W. Victor
Reg. No. 39,867

Dated: January 10, 2007

Direct All Correspondence to:
David Victor
Konrad Raynes & Victor LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, California 90212
Tel: 310-553-7977
Fax: 310-556-7984

IX. Claims Appendix

1. (Previously Presented) A method for enabling access to data in a storage medium within one of a plurality of storage cartridges enabled to be mounted into an interface device, comprising:

providing an association of at least one coding key to the plurality of storage cartridges;

encrypting the coding key; and

decrypting the encrypted coding key to use to decode and code data stored in the storage medium of at least one of the storage cartridges.

2. (Original) The method of claim 1, further comprising:

using the coding key to encode data to write to the storage medium;

transmitting the encoded data to the interface device to write to the storage medium in one storage cartridge mounted in the interface device;

receiving encoded data from the interface device read from the storage medium; and

using the coding key to decrypt the received encoded data.

3. (Previously Presented) The method of claim 1, wherein the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key is enabled to encode data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

4. (Original) The method of claim 1, wherein the association of the at least one coding key to the plurality of storage cartridges associates a different key with each storage cartridge, wherein the key associated with one storage cartridge is used to encode data written to the storage medium and decode data read from the storage medium of the storage cartridge.

5. (Original) The method of claim 1, wherein the coding key comprises a seed value that is used to generate an additional key that is used to directly decode and encode the data in the storage medium in the storage cartridge.

6. (Original) The method of claim 1, further comprising:

transmitting the encrypted coding key to the interface device, wherein the interface device decrypts the coding key to use to decode and code data stored in the storage medium.

7. (Previously Presented) The method of claim 6, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein a second key used by the interface device enabled to decrypt the coding key encrypted with the first key.

8. (Previously Presented) The method of claim 6, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein a second key enabled to decrypt the coding key encrypted with the first key;

encrypting the second key with a third key, wherein a fourth key used by the interface device enabled to decrypt data encrypted with the third key; and

transmitting the coding key encrypted with the first key and the second key encrypted with the third key to the interface device.

9. (Previously Presented) The method of claim 6, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein a second key enabled to decrypt the coding key encrypted with the first key;

transmitting the coding key encrypted with the first key to the interface device;

receiving, from the interface device, the coding key encrypted with the first key;

decrypting the coding key with the second key;

encrypting the coding key with a third key, wherein a fourth key used by the interface device enabled to decrypt data encrypted with the third key; and

transmitting the coding key encrypted with the third key to the interface device.

10. (Previously Presented) A method performed by an interface device for accessing data in a removable storage cartridge including a storage medium coupled to the interface device, comprising:

receiving an encrypted coding key from a host system;

decrypting the encrypted coding key;

using the coding key to encode data to write to the storage medium; and

using the coding key to decode data written to the storage medium.

11. (Original) The method of claim 10, wherein encoding the data with the coding key compresses the data and wherein decoding the data written to the storage medium decompresses the data, and wherein the data can only be encoded or decoded using the coding key.

12. (Previously Presented) The method of claim 10, wherein the coding key is encrypted by a first key maintained at the host system, further comprising;

maintaining a second key that enabled to decrypt data encrypted using the first key, wherein the second key is used to decrypt the coding key encrypted with the first key.

13. (Original) The method of claim 12, wherein the second key is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key.

14. (Original) The method of claim 13, further comprising:

transmitting the coding key decrypted using the decrypting logic to encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to encode and decode data to the storage medium.

15. (Original) The method of claim 12, further comprising:

storing the coding key encrypted with the first key within the storage cartridge;

receiving an input/output (I/O) request directed to the storage cartridge; and

accessing the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

16. (Previously Presented) The method of claim 10, wherein the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key that is enabled to decrypt data encrypted using the first key, further comprising:

receiving, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is decrypted using a fourth key;

accessing the fourth key;

using the fourth key to decrypt the encrypted second key received from the host system; and

using the decrypted second key to decrypt the received coding key encrypted using the first key.

17. (Previously Presented) The method of claim 10, wherein the coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key that is enabled to decrypt data encrypted using the first key, further comprising:

transmitting the encrypted coding key received from the host system back to the host system; and

in response to transmitting the encrypted coding key back to the host system, receiving, from the host system, the coding key encrypted using a third key, wherein data encrypted using the third key is decrypted using a fourth key; and

accessing the fourth key, wherein the coding key is decrypted using the fourth key.

18. (Previously Presented) A system for enabling access to data in a storage medium within one of a plurality of storage cartridges, comprising:

an interface device at which the storage cartridges are enabled to be mounted, wherein the interface device is enabled to write data to the storage medium within the storage cartridges and reading data from the storage medium in the storage cartridges;

means for providing an association of at least one coding key to the plurality of storage cartridges;

means for encrypting the coding key; and

decrypting the encrypted coding key to use to decode and encode data stored in the storage medium of at least one of the storage cartridges.

19. (Original) The system of claim 18, further comprising:

means for using the coding key to encode data to write to the storage medium;

means for transmitting the encoded data to the interface device to write to the storage medium in one storage cartridge mounted in the interface device;

means for receiving encoded data from the interface device read from the storage medium; and

means for using the coding key to decrypt the received encoded data.

20. (Previously Presented) The system of claim 18, wherein the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key is enabled to be used to encode data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

21. (Original) The system of claim 18, wherein the association of the at least one coding key to the plurality of storage cartridges associates a different key with each storage cartridge, wherein the key associated with one storage cartridge is used to encode data written to the storage medium and decode data read from the storage medium of the storage cartridge.

22. (Original) The system of claim 18, further comprising:

means for transmitting the encrypted coding key to the interface device, wherein the interface device decrypts the coding key to use to decode and code data stored in the storage medium.

23. (Previously Presented) A system for accessing data in a removable storage cartridge including a storage medium, wherein the system is in communication with a host system, comprising:

an interface device enabled to be coupled to the removable storage cartridge to access data in the removable storage cartridge, wherein the interface device causes operations to be performed, comprising:

receiving an encrypted coding key from the host system;

decrypting the encrypted coding key;

using the coding key to encode data to write to the storage medium; and

using the coding key to decode data written to the storage medium.

24. (Previously Presented) The system of claim 23, wherein the coding key is encrypted by a first key maintained at the host system, wherein the interface device further causes operations comprising;

maintaining a second key that is enabled to decrypt data encrypted using the first key, wherein the second key is used to decrypt the coding key encrypted with the first key.

25. (Previously Presented) The system of claim 24, wherein the interface device further includes:

an integrated circuit non-volatile memory including the second key, wherein the integrated circuit non-volatile memory;

decrypting logic for using the second key to decrypt data encrypted using the first key, wherein the integrated circuit non-volatile memory is only accessible to the decrypting logic.

26. (Previously Presented) The system of claim 24, wherein the interface device further causes operations comprising:

storing the coding key encrypted with the first key within the storage cartridge;

receiving an input/output (I/O) request directed to the storage cartridge; and

accessing the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

27. (Previously Presented) An article of manufacture including code for enabling access to data in a storage medium within one of a plurality of storage cartridges enabled to be mounted into an interface device, wherein the code is enabled to cause operations comprising:

providing an association of at least one coding key to the plurality of storage cartridges;

encrypting the coding key; and

decoding the encrypted coding key to use to decode and code data stored in the storage medium of the at least one storage cartridge.

28. (Original) The article of manufacture of claim 27, further comprising:

using the coding key to encode data to write to the storage medium;

transmitting the encoded data to the interface device to write to the storage medium in one storage cartridge mounted in the interface device;

receiving encoded data from the interface device read from the storage medium; and

using the coding key to decrypt the received encoded data.

29. (Previously Presented) The article of manufacture of claim 27, wherein the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key is enabled to encode data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

30. (Original) The article of manufacture of claim 27, wherein the association of the at least one coding key to the plurality of storage cartridges associates a different key with each storage cartridge, wherein the key associated with one storage cartridge is used to encode data written to the storage medium and decode data read from the storage medium of the storage cartridge.

31. (Original) The article of manufacture of claim 27, wherein the coding key comprises a seed value that is used to generate an additional key that is used to directly decode and encode the data in the storage medium in the storage cartridge.

32. (Original) The article of manufacture of claim 27, further comprising:

transmitting the encrypted coding key to the interface device, wherein the interface device decrypts the coding key to use to decode and code data stored in the storage medium.

33. (Previously Presented) The article of manufacture of claim 32, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein a second key used by the interface device is enabled to decrypt the coding key encrypted with the first key.

34. (Previously Presented) The article of manufacture of claim 32, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein a second key is enabled to decrypt the coding key encrypted with the first key;

encrypting the second key with a third key, wherein a fourth key used by the interface device is enabled to decrypt data encrypted with the third key; and

transmitting the coding key encrypted with the first key and the second key encrypted with the third key to the interface device.

35. (Previously Presented) The article of manufacture of claim 32, wherein encrypting the coding key further comprises:

encrypting the coding key with a first key, wherein a second key is enabled to decrypt the coding key encrypted with the first key;

transmitting the coding key encrypted with the first key to the interface device;

receiving, from the interface device, the coding key encrypted with the first key;

decrypting the coding key with the second key;

encrypting the coding key with a third key, wherein a fourth key used by the interface device is enabled to decrypt data encrypted with the third key; and

transmitting the coding key encrypted with the third key to the interface device.

36. (Previously Presented) An article of manufacture including code executed in an interface device for accessing data in a removable storage cartridge including a storage medium coupled to the interface device, wherein the interface device is in communication with a host system, and wherein the code causes operations comprising:

receiving an encrypted coding key from the host system;

decrypting the encrypted coding key;

using the coding key to encode data to write to the storage medium; and

using the coding key to decode data written to the storage medium.

37. (Original) The article of manufacture of claim 36, wherein encoding the data with the coding key compresses the data and wherein decoding the data written to the storage medium decompresses the data, and wherein the data can only be encoded or decoded using the coding key.

38. (Previously Presented) The article of manufacture of claim 36, wherein the coding key is encrypted by a first key maintained at the host system, further comprising;

maintaining a second key that is enabled to decrypt data encrypted using the first key, wherein the second key is used to decrypt the coding key encrypted with the first key.

39. (Original) The article of manufacture of claim 38, wherein the second key is stored in an integrated circuit non-volatile memory that is only accessible to decrypting logic that uses the second key to decrypt data encrypted using the first key.

40. (Original) The article of manufacture of claim 36, further comprising:

transmitting the coding key decrypted using the decrypting logic to encoder/decoder logic, wherein the encoder/decoder logic uses the coding key to encode and decode data to the storage medium.

41. (Original) The article of manufacture of claim 38, further comprising:

storing the coding key encrypted with the first key within the storage cartridge;

receiving an input/output (I/O) request directed to the storage cartridge; and

accessing the encrypted coding key from the storage cartridge, wherein the accessed coding key is decrypted using the second key, and wherein the decrypted coding key is used to encode and decode data to execute the I/O request to the storage cartridge.

42. (Previously Presented) The article of manufacture of claim 36, wherein the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key that is enabled to decrypt data encrypted using the first key, further comprising:

receiving, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is enabled to be decrypted using a fourth key;

accessing the fourth key;

using the fourth key to decrypt the encrypted second key received from the host system; and

using the decrypted second key to decrypt the received coding key encrypted using the first key.

43. (Previously Presented) The article of manufacture of claim 36, wherein the coding key is encrypted by a first key maintained at the host system, wherein the host

system maintains a second key that is enabled to decrypt data encrypted using the first key, further comprising:

transmitting the encrypted coding key received from the host system back to the host system; and

in response to transmitting the encrypted coding key back to the host system, receiving, from the host system, the coding key encrypted using a third key, wherein data encrypted using the third key is decrypted using a fourth key; and

accessing the fourth key, wherein the coding key is decrypted using the fourth key.

X. Evidence Appendix

None

XI. Related Proceedings Appendix

None